Ekwan E. Rhow – State Bar No. 174604
Marc E. Masters – State Bar No. 208375
Christopher J. Lee – State Bar No. 322140
BIRD, MARELLA, BOXER, WOLPERT, NESSIM,
DROOKS, LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100

Jonathan M. Rotter – State Bar No. 234137
Kara M. Wolke – State Bar No. 241521
Gregory B. Linkh – pro hac vice forthcoming
GLANCY PRONGAY & MURRAY, LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150

Kalpana Srinivasan – State Bar No. 237460
Steven Sklaver – State Bar No. 237612
Michael Gervais – State Bar No. 330731
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles CA 90067
Telephone: (310) 789-3100

Attorneys for Plaintiff Bernadine Griffith

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH, individually and on behalf of all others similarly situated, Plaintiff, vs. TIKTOK, INC., a corporation; BYTEDANCE, INC., a corporation Defendants.	CASE NO. 5:23-cv-964 **CLASS ACTION COMPLAINT FOR:** **(1) Violation of the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.*** **(2) Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*** **(3) Statutory Larceny under Cal. Pen. Code §§ 484, 496** **(4) Conversion** **(5) Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*** **(6) Invasion of Privacy under Article**

I, Section 1 of the California Constitution
(7) Intrusion upon Seclusion

DEMAND FOR JURY TRIAL

Plaintiff Bernadine Griffith, individually and on behalf of all others similarly situated, files this Class Action Complaint against defendants TikTok Inc. and ByteDance Inc. (collectively, "Defendants"), and in support states the following:

I. INTRODUCTION

1. This case is about the Defendants' unauthorized interception, collection, saving and use of non-TikTok users' highly personal data whenever the non-TikTok users visit a website with the TikTok SDK installed. Defendants engaged in this conduct even where non-TikTok users employed privacy settings that are meant to block third-party tracking of their web activity. This conduct is Defendants' latest salvo in their ongoing campaign to illicitly harvest an enormous amount of private data on U.S. residents.

2. Since its introduction in 2017 as the international version of the Chinese social video app Douyin, TikTok has taken the United States – and the world – by storm. As of 2022, over 1 billion people worldwide and 100 million people in the United States signed up for the TikTok app to create, view, and share short videos popularized by the platform. The success of the TikTok app has allowed its ultimate owner, Beijing ByteDance Technology Co. Ltd. ("Beijing ByteDance"), to grow from a small Chinese technology company to a multibillion-dollar international conglomerate.

3. But while Defendants TikTok Inc. and ByteDance Inc. (as well as non-party Beijing ByteDance) may have risen to prominence based on the viral videos of adorable puppies and trendy dance moves shared on the TikTok app, they have also become infamous for something far more sinister: invasive and non-consensual harvesting of private user information. Defendants paid $5.7 million to settle

allegations by the federal government that they were stealing private information from children. And Defendants paid a $92 million class action settlement relating to allegations that they illicitly made face geometry scans and took private data from millions of U.S. TikTok app users without consent – making all such data available in China, where companies are obligated by law to assist the Chinese Communist Party with intelligence gathering.[1]

4. It is no exaggeration to say that Defendants and their TikTok app are a clear and present danger to personal privacy. Accordingly, many U.S. residents have elected to abstain from using the TikTok app, including many parents who have also taken up the difficult task of keeping their children off the platform for their own safety. As of the time of this filing, Congress is discussing a bill – that has garnered bipartisan support – that would ban the use of the TikTok app nationwide.[2]

5. Unfortunately, a ban on the TikTok app itself would not solve the problem, because Defendants intercept and collect private data from U.S. residents browsing third-party websites—***including U.S. residents who never even used the TikTok app.*** While U.S. residents browse completely unrelated websites to watch their favorite television show, search for medical information, or purchase a birthday gift for their children, TikTok software owned by Defendants and installed on those websites – the "TikTok SDK" – secretly intercepts and collects their private data and sends it to Defendants. The TikTok SDK is marketed as an enterprise solution for websites to identify users and deliver targeted ads. Unknown to users of these websites, however, the TikTok SDK intercepts and collects sensitive private data and delivers it to Defendants while performing its advertised function.

[1] https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (China's National Intelligence Law "repeatedly obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of 'intelligence' work")

[2] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998

6. In sum, the TikTok SDK has become yet another, even more insidious, means through which Defendants steal private data from U.S. residents. The purpose of this lawsuit is to put an end to this practice and compensate those injured to the fullest extent of the law.

II. THE PARTIES

A. The Plaintiff

7. Plaintiff Bernadine Griffith is, and at all relevant times was, an individual and resident of Riverside County, California.

B. The Defendants

8. Defendant TikTok, Inc. f/k/a Musical.ly, Inc. ("TikTok, Inc.") is, and at all relevant times was, a California corporation with its principal place of business in Culver City, California. Defendant TikTok, Inc. also maintains offices in Palo Alto, California and Mountain View, California. The name change from Musical.ly, Inc. to TikTok, Inc. occurred in May 2019. Defendant TikTok, Inc. is a wholly-owned subsidiary of TikTok, LLC, which in turn is a wholly-owned subsidiary of TikTok, Ltd. And TikTok, Ltd. is a wholly owned subsidiary of ByteDance, Ltd., a Cayman Islands corporation which is headquartered in Beijing, China.

9. Defendant ByteDance, Inc. ("ByteDance") is, and at all relevant times was, a Delaware corporation with its principal place of business in Palo Alto, California. Defendant ByteDance, Inc. is also a wholly-owned subsidiary of ByteDance, Ltd.

C. Alter Ego and Single Enterprise Allegations

10. At all relevant times, Defendants have shared offices in Silicon Valley and also have shared employees. Employees of both companies have performed work on and concerning the TikTok SDK that is at the center of this lawsuit.

11. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer, and/or alter ego of the other Defendant, and acted in the course and scope of such agency, partnership,

and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and/or participated in the acts or transactions of the other Defendant.

12. At all relevant times, and in connection with the matters alleged herein, Defendants were controlled and largely owned by the same person, Beijing ByteDance founder Zhang Yiming, and constitute a single enterprise with a unity of interest. Recognition of the privilege of separate existence under such circumstances would promote injustice.

III. JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1332(d) & 1367 because (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens of states different from some Defendants.

14. This Court has personal jurisdiction over Defendants because (i) they are headquartered and/or incorporated in this District, (ii) transact business in this District; (iii) they have substantial aggregate contacts in this District; and (iv) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons in this District.

15. In accordance with 28 U.S.C. § 1391, venue is proper in this District because (i) a substantial part of the conduct giving rise to the claims occurred in and/or emanated from this District; (ii) Defendants transact business in this District; (iii) one Defendant has its principal place of business in this District; and (iv) one Defendant has offices in this District.

IV. GENERAL ALLEGATIONS

A. Defendants' history of misappropriating user data through the TikTok app

16. Beijing ByteDance was founded in 2012 and operates a variety of social networking and news applications, which it regards as "part of an artificial intelligence company powered by algorithms that 'learn' each user's interests and preferences through repeat interaction."[3] As a relative latecomer to the Chinese tech industry, Beijing ByteDance was initially forced to look to overseas markets, including the United States.[4] Eventually, this view toward international expansion allowed the company to grow at a scale far beyond its peers: as of 2022, Beijing ByteDance had become China's foremost technology conglomerate, valued at approximately $300 billion.[5] Most of Beijing ByteDance's revenue is derived from advertising through its various software and app offerings.[6]

17. Internationally, Beijing ByteDance is most well-known for the TikTok app, a "global phenomenon" with a massive American audience.[7] Starting from a global user base of 55 million in January 2018, TikTok has grown at a staggering rate, passing 1 billion users in September 2021.[8]

18. This meteoric rise has led to a rapid expansion in Defendants' U.S. presence. In 2019, Defendant TikTok, Inc. took over office space in Silicon Valley once occupied by Facebook's WhatsApp messaging app, and began poaching

[3] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated-for-national-securitythreats; https://www.cotton.senate.gov/?p=press_release&id=1239

[4] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-isserious-11561780861

[5] https://www.scmp.com/tech/big-tech/article/3193027/tiktok-owner-bytedance-sees-valuation-drop-quarter-us300-billion

[6] https://www.bloomberg.com/news/articles/2019-01-15/bytedance-is-said-to-hit-lower-end-ofsales-goal-amid-slowdown.

[7] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/

[8] https://www.cnbc.com/2021/09/27/tiktok-reaches-1-billion-monthly-users.html

employees from American rivals including Facebook, Snap, Hulu, Apple, YouTube, and Amazon, offering salaries as much as 20% higher.[9]

19. One key to Defendants' financial success was the targeted advertising they ran through the TikTok app, which was made possible through an illicit and highly-invasive data harvesting campaign. Through this campaign, Defendants unlawfully accumulated private and personally-identifiable information on TikTok users, which Defendants aggregated and monetized to unjustly profit from their unlawful activities.

20. On February 27, 2019, in response to a complaint filed by the FTC, Defendant TikTok, Inc. (at the time known as Musical.ly Inc.) stipulated to an order mandating a civil penalty in the amount of $5.7 million and injunctive relief concerning their unlawful collection of personal information from children through Musical.ly (the predecessor to the TikTok app) – the largest ever civil penalty of its kind.[10] The subsequent FTC statement indicated that these practices "reflected the company's willingness to pursue growth even at the expense of endangering children."[11]

21. In 2022, Defendants paid $92 million to settle a class action lawsuit alleging that it had been scanning the faces and voices of its users and transferring them to databases controlled by China-based third parties.[12] Immediately after the settlement, Defendants amended their privacy policy to force users to consent to the

[9] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html

[10] *United States of America v. Musical.ly and Musical.ly, Inc.*, United States District Court,
Central District of California, Case No. 2:19-cv-1439

[11] https://www.nbcnews.com/tech/tech-news/tiktok-pay-5-7-million-over-alleged-violation-childprivacy-n977186

[12] https://www.cnbc.com/2022/10/28/tiktok-users-paid-over-privacy-violations-google-snap-could-be-next.html

collection of biometric information.[13] Alessandro Acquisti, a professor of technology policy at Carnegie Mellon University, assessed that this biometric data collection could potentially be put to "chilling" uses, including "mass re-identification and surveillance."[14]

22. On August 6, 2020, then-President Donald Trump issued an executive order banning the download and use of the TikTok app within the United States, on the grounds that it "automatically captures vast swaths of information from its users, including Internet and other network activity information such as location data and browsing and search histories" and "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information — potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[15]

23. While this Executive Order was never enforced, concerns regarding the potential privacy and national security implications of Defendants' U.S. business have only increased. In December of 2022, President Joe Biden signed into law a bill banning the use of the TikTok app on devices used by the federal government's nearly 4 million employees.[16] Media reports also indicate that "momentum is building" within Congress for a complete nationwide ban on the TikTok app.[17] State legislatures have separately been debating a ban on the TikTok app as well, and Montana became the first state to pass a ban in May, 2023.[18]

[13] https://time.com/6071773/tiktok-faceprints-voiceprints-privacy/

[14] *Id.*

[15] https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

[16] https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724

[17] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998

[18] https://www.cnn.com/2023/04/14/tech/montana-house-tiktok-ban/index.html; https://www.cnn.com/2023/05/17/tech/montana-governor-tiktok/index.html

24. In February 2023, Senators Richard Blumenthal and Jerry Moran signed a joint letter demanding that the government impose a wall between Defendant TikTok Inc.'s U.S. operations and its Chinese parent company, Beijing ByteDance.[19] Senator Michael Bennet has urged TikTok Inc.'s CEO Shou Zi Chew "to consider his platform's harm to a generation of Americans."[20] Senate majority leader Chuck Schumer has indicated that the Senate Commerce Committee is currently conducting a review of the TikTok app and that a ban on the TikTok app "should be looked at."[21]

25. Unsurprisingly, the American public has grown increasingly distrustful of Defendants' business practices. 59% of respondents to a February 2023 Harvard CAPS/Harris national poll said they believed that the TikTok app "is a medium the Chinese use to spy on Americans."[22] 42% said they would support a nationwide TikTok ban on privacy and security grounds.[23] Only 12% said they would allow the continued use of the TikTok app in the United States without conditions.[24]

B. Cookies and SDKs

26. The TikTok SDK represents the next step in Defendants' data harvesting campaign aimed at U.S. residents. Defendants have developed software that can and does illicitly harvest private and personally-identifiable data, such as the webpages visited by users, search queries, User IDs, User Agent, phone numbers, email addresses, IP addresses, and more (collectively "Private Data") from users of websites with the TikTok SDK installed. Defendants have the ability to invade the privacy of unsuspecting U.S. residents who do not use the TikTok app, as these non-

[19] https://www.nbcnews.com/politics/congress/congress-tiktok-ban-social-media-harms-teens-rcna70998

[20] *Id.*

[21] https://www.cnn.com/2023/02/12/tech/tiktok-us-ban-consideration-chuck-schumer/index.html

[22] https://harvardharrispoll.com/key-results-february-3/

[23] *Id.*

[24] *Id.*

TikTok users go about their everyday business on websites that have no visible affiliation whatsoever to Defendants.

27. An SDK – short for "software development kit" – is a package of pre-built software tools that allows developers to implement certain functionality on their platforms without the need to re-build code from the ground up.

28. Much modern software leverages SDKs from large software companies such as Google, Apple, or Microsoft, so that developers can implement basic functions "out of the box" with a simple download and installation, rather than having to "reinvent the wheel" every time for new software. For example, an "in-app billing" SDK can be used to implement billing functions, and an "advertising" SDK can be used to display ads on websites.

29. In particular, SDKs have become increasingly popular for web advertising. Once installed onto a particular website, advertising SDKs allow a website to connect to a larger ad network – such as Google AdSense or Facebook Ads – which allows them to serve personalized ads to users, and also collect some user data to send back to the ad network. Websites are compensated in the form of a share of the ad revenue from the network, based on the amount of traffic driven from the website to the network's ads.

30. Advertising SDKs can deliver personalized ads because they collect user data through "cookies." Cookies are small computer files that are automatically generated when a user visits a website, comprised of strings of text that contain information, such as user IDs, emails, or IP addresses. Every time a user visits the website, the cookie on the user's hard drive is passed back to the website for identification purposes. Cookies were originally developed to enable basic functionality requiring user identification, such as automatic log-ins, or saving your shopping cart on an e-commerce website. As technology has advanced, however, so too has the scope of the information collected by cookies.

31. In general, cookies are categorized by (1) the length of time for which they are placed on a user's device, and (2) the party who places the cookie on the user's device. "Session cookies" are placed on the user's computer for the time period in which the user is reading and navigating the website that placed the cookie. Web browsers normally delete session cookies when the user closes the browser. "Persistent cookies" are designed to survive past one browser session of a user. The lifespan of a persistent cookie is set by the person who creates the cookie. As a result, a "persistent cookie" could stay on a user's device for years. Persistent cookies can be used to track users' actions on the Internet, and are also sometimes referred to as "tracking cookies."

C. Defendants use the TikTok SDK to secretly intercept and collect Private Data from unsuspecting U.S. residents browsing websites seemingly unrelated to TikTok

32. The TikTok SDK is a new enterprise solution developed by Defendants and distributed under their "TikTok for Business" product line. Defendants market the TikTok SDK as a means to deliver more effective targeted ads – thus increasing ad revenue for websites that choose to install the TikTok SDK.

33. When a user visits a website that has the TikTok SDK installed, two cookies are downloaded onto the user's hard drive: a "first-party" cookie that is initially accessible by only the website, and a "third-party" cookie that is accessible directly by Defendants. These cookies store a broad range of personal information, including email addresses, phone numbers, user IDs, browsing histories, and search queries.

34. The "third-party" cookies are downloaded onto a user's computing device from each website where the TikTok SDK is installed, allowing Defendants to keep track of and monitor an individual user's web activity over multiple websites.

35. Third-party cookies are used to help create detailed profiles on individuals, including but not limited to an individual's unique ID number, IP

address, browser, screen resolution, search terms and a history of all websites visited within Defendants' TikTok SDK network of websites. This allows Defendants to track the web activity of an individual and build a digital dossier.

36. The TikTok SDK also allows sites to utilize a "Pixel", which is a piece of JavaScript code placed on the website with the TikTok SDK which tracks user behavior. According to TikTok's own documentation, TikTok Pixel collects the following information:

- **Ad/Event information:** Information about the ad a TikTok user has clicked or an event that was triggered.
- **Timestamp:** Time that the pixel event fired. This is used to determine when website actions took place, like when a page was viewed, when a product was purchased, etc.
- **IP Address:** Used to determine the geographic location of an event.
- **User Agent:** Used to determine the device make, model, operating system, and browser information.
- **Cookies:** First-party cookies are optional but third-party cookies are on by default with the TikTok Pixel. Cookies help the measurement, optimization, and targeting of your campaigns. Performance is boosted when first- and third-party cookies are paired with Advanced Matching.[25]

37. Web browsers – such as Apple Safari, Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox – have privacy settings that provide users the ability to block third-party cookies. For example, under the "Privacy and Security" settings in Google Chrome, users have the option to "Block third-party cookies."

38. Yet, where a web browser or operating system is set to block third-party cookies to prevent Defendants from obtaining Private Data, Defendants circumvent

[25] https://ads.tiktok.com/help/article/tiktok-pixel?redirected=2

those settings to obtain Private Data anyway. The TikTok SDK circumvents web browser and system settings by causing the website to share the first-party cookie with Defendants, in effect transmuting a first-party cookie into a third-party cookie with the ability to evade web browser and operating system settings that would otherwise block it from reaching Defendants.

39. A large number of widely-used websites have installed the TikTok SDK, thereby allowing Defendants to obtain Private Data from users of these websites. Having never used the TikTok app or registered for a TikTok account, a multitude of users of these websites never had any notice—actual or constructive—of TikTok's privacy policy or terms of use, and never consented to Defendants' interception and collection of the users' Private Data. By aggregating Private Data over a wide range of websites, Defendants assemble a comprehensive profile of these non-TikTok users.

40. For example, CONSUMER REPORTS recently revealed that:

> The national Girl Scouts website has a TikTok pixel on every page, which will transmit details about children if they use the site. TikTok gets medical information from WebMD, where a pixel reported that we'd searched for "erectile dysfunction." And RiteAid told TikTok when we added Plan B emergency contraceptives to our cart. Recovery Centers of America, which operates addiction treatment facilities, notifies TikTok when a visitor views its locations or reads about insurance coverage.[26]

41. The TikTok SDK and TikTok Pixel can also be used for purposes of digital "fingerprinting." As explained by WIRED:

> The exact configuration of lines and swirls that make up your fingerprints are thought to be unique to you. Similarly, your browser fingerprint is a set of information that's collected from your phone or laptop each time you use it that advertisers can eventually link back to you.
>
> "It takes information about your browser, your network, your device and combines it together to create a set of characteristics that is mostly unique to you," says Tanvi Vyas, a principal engineer at Firefox. The

[26] https://www.consumerreports.org/electronics-computers/privacy/tiktok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/

> data that makes up your fingerprint can include the language you use, keyboard layout, your timezone, whether you have cookies turned on, the version of the operating system your device runs, and much more.
>
> By combining all this information into a fingerprint, it's possible for advertisers to recognize you as you move from one website to the next. Multiple studies looking at fingerprinting have found that around 80 to 90 percent of browser fingerprints are unique. Fingerprinting is often done by advertising technology companies that insert their code onto websites. Fingerprinting code—which comes in the form of a variety of scripts, such as the FingerprintJS library—is deployed by dozens of ad tech firms to collect data about your online activity. Sometimes websites that have fingerprinting scripts on them don't even know about it. And the companies are often opaque and unclear in the ways they track you.
>
> Once established, someone's fingerprint can potentially be combined with other personal information—such as linking it with existing profiles or information murky data brokers hold about you. "There are so many data sets available today, and there are so many other means to connect your fingerprint with other identifying information," says Nataliia Bielova, a research scientist at France's National Institute for Research in Digital Science and Technology, who is currently working at the French data regulator, CNIL.[27]

42. Upon information and belief, Defendants are able to associate the information they obtain through the unconsented to and undisclosed data collection described herein with personally identifying information of non-TikTok users. Defendants are able to accomplish this through, among other things, "digital fingerprinting" techniques.

43. Defendants' audacious invasion of privacy without notice to or the authorization of Plaintiff and Class and Subclass members is motivated, in part, by its effort to improve its own algorithms and technology. The explosive growth in the popularity of the TikTok app – and attendant growth in advertising revenue for Defendants – is attributable, in part, to the TikTok app's ability to predict the interests of its users. This capability is powered by an algorithm that has benefited from a mountain of data – regardless of whether it comes from TikTok or non-TikTok users – collected by Defendants. Defendants use the illicitly collected data to improve their

[27] https://www.wired.com/story/browser-fingerprinting-tracking-explained/

own algorithms and technology. Websites from which Defendants surreptitiously intercept and collect Private Data through the TikTok SDK include such popular and widely-known websites as streaming video service Hulu, e-commerce platform Etsy, media company Telemundo, freelancing platform Upwork, and Build-a-Bear Workshop, a custom teddy bear design shop for children. These are just a few examples of the countless websites that have become Trojan horses for Defendants to steal Private Data from non-TikTok users in the United States.

D. Plaintiff's and Class and Subclass members' Private Data has economic value, and there is a market for such Private Data

44. The value of personal data is well understood and generally accepted as a form of currency.

45. It is by now incontrovertible that a robust market for this data undergirds the tech economy.

46. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[28] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[29] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

47. The Organization for Economic Cooperation and Development ("OECD") itself has published numerous volumes discussing how to value data such as that which is the subject matter of this Complaint, including as early as 2013, with its publication "Exploring the Economic of Personal Data: A Survey of Methodologies for Measuring Monetary Value".[30] The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big

[28] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[29] https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

[30] http://dx.doi.org/10.1787/5k486qtxldmq-en

data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."[31]

48. In *The Age of Surveillance Capitalism*, Harvard Business School Professor Shoshanna Zuboff notes that large corporations like Verizon, AT&T and Comcast have transformed their business models from fee for services provided to customers to monetizing their user's data—including user data that is not necessary for product or service use, which she refers to as "behavioral surplus."[32] In essence, Professor Zuboff explains that revenue from Internet user data pervades every economic transaction in the modern economy. It is a fundamental assumption of these revenues that there is a *market* for this data; data generated by Internet users on websites in which the TikTok SDK is installed has economic value.

49. Professor Paul M. Schwartz, writing in the Harvard Law Review, notes: "Personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing, and corporate America is moving quickly to profit from the trend. Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information."[33]

50. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis, and use. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiff herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[34] Likewise, apps

[31] https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en

[32] Shoshanna Zuboff, *The Age of Surveillance Capitalism* 166 (2019)

[33] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2055, 2056-57 (2004)

[34] https://wallethacks.com/apps-for-selling-your-data/

such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.[35]

51. There are countless examples of this kind of market, which is growing more robust as information asymmetries are diminished through revelations to users as to how their data is being collected and used.

52. As Professors Acquisti, Taylor and Wagman relayed in their 2016 article "The Economics of Privacy", published in the *Journal of Economic Literature*: "Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties."[36]

53. There is also a private market for Internet users' personal information. While there is a wide range in values, the prices are nonetheless significant. For example:

- "Each piece of personal info has a price tag. A Social Security number may sell for as little as $1. Credit card, debit card and banking info can go for as much as $110. Usernames and passwords for non-financial institution logins are $1, but it can range from $20 to $200 for login info for online payment platforms."[37]
- "Researchers pored through the prices of personal data and information—called 'fullz' by those searching for 'full credentials'—that are available for sale on nearly 50 different Dark Web marketplaces, finding that Japan, the UAE, and EU countries have the most expensive identities available at an average price of $25."[38]

[35] https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-bytedance-rival

[36] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, *The Economics of Privacy*, 54 J. of Econ. Literature 2, at 444 (June 2016), https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf

[37] https://www.onpointcu.com/blog/understanding-the-illegal-market-for-personal-information/#:~:text=Each%20piece%20of%20personal%20info,info%20for%20online%20payment%20platforms

[38] https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-dark-web-for-americans-its-just-8/

- "According to Comparitech, who researched the prices of stolen credit cards, hacked PayPal accounts, and private Social Security numbers on more than 40 different dark web marketplaces, the average price of each U.S. citizen's "fullz," or complete information including name, date of birth, address, phone number, account numbers and other information is $8."[39]

54. These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

55. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

E. Plaintiff and Class and Subclass members suffered an economic injury.

56. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications.

57. California courts have recognized the lost "property value" of personal information. Recent changes in California law have also confirmed that individuals have a property interest in their information. In 2018, California enacted the California Consumer Privacy Act ("CCPA"). Among other things, the CCPA permits businesses to purchase consumer information from consumers themselves (Cal. Civ. Code § 1798.125(b)(1)) and permits businesses to assess and appraise – *i.e.*, to place a monetary value on – consumer data (Cal. Civ. Code § 1798.125(a)(2)).

58. Accordingly, Plaintiff's and Class and Subclass members' Private Data is property under California law.

59. Defendants' interception, collection, and use of Plaintiff's and Class and Subclass members' Private Data without authorization is a taking of Plaintiff's and Class and Subclass members' property. Plaintiff and Class and Subclass members

[39] https://vmits.com/theres-value-in-everything-stop-underestimating-the-value-of-your-data-on-the-black-market/

have a right to disgorgement and/or restitution damages for the value of the improperly collected Private Data by Defendants through the TikTok SDK.

60. Plaintiff and Class and Subclass members have suffered benefit of the bargain damages, in that Defendants took more data than authorized. Those benefit of the bargain damages also include, but are not limited to (i) loss of the promised benefits of their experience on the websites on which the TikTok SDK is installed; (ii) out-of-pocket costs; and (iii) loss of control over property which has marketable value.

61. To preserve their privacy, Plaintiff and Class and Subclass members who now understand at least some of Defendants' violations are presented with the choice of (i) reducing or ending their participation with the websites on which the TikTok SDK is installed; or (ii) knowingly accepting less privacy than they were promised. Each of these options deprives Plaintiff and Class and Subclass members of the benefits of their original bargain. There is no option that recovers the property improperly intercepted and collected by Defendants.

62. Further, Plaintiff and Class and Subclass members were denied the benefit of knowing that Defendants were intercepting and collecting their Private Data. Thus, they were unable to mitigate the harms they incurred because of Defendants' actions. That is, Defendants' lack of transparency prevented and still prevents Plaintiff's and Class and Subclass members' ability to mitigate the harms.

63. Defendants avoided costs they should have incurred because of their actions—had they transparently disclosed their actions, they would have suffered losses stemming from the third-party websites' loss of user engagement. Warning users would have chilled engagement on the third-party websites as well as discouraged potential new users, and thus chilled use of the TikTok SDK.

64. Defendants thus were not only able to evade or defer these costs, but they were able to continue to accrue value and further benefit from the delay due to the time value of money. Defendants have thus transferred all of the costs imposed

by the unauthorized interception and collection of users' Private Data onto Plaintiff and Class and Subclass members. Defendants increased the cost to Plaintiff and Class and Subclass members of mitigating the interception and collection of their Private Data by failing to notify them that Defendants were intercepting and collecting Plaintiff's and Class and Subclass members' Private Data.

65. In addition, Plaintiff and Class and Subclass members have suffered from the diminished value of their own Private Data, which is property that has both personal and economic value to Plaintiff and Class and Subclass members.

66. Plaintiff's and Class and Subclass members' Private Data have different forms of value. First, there is transactional, or barter, value. Indeed, Defendants have traded (i) the ability to use those websites with the TikTok SDK installed in exchange for (ii) the collection and use of Plaintiff's and Class and Subclass members' Private Data—all while concealing the extent to which this information would be intercepted, collected, and used.

67. Second, Plaintiff's and Class and Subclass members' property, which has economic value, was taken from them without their consent. There is a market for this Private Data, and it has at minimum a value greater than zero. Plaintiff and Class and Subclass members cannot bring their Private Data to market because Defendants' improper interception, collection, and use of that Private Data for particular advertising purposes means that Plaintiff's and Class and Subclass members' Private Data is no longer needed or marketable for that purpose.

68. Third, in addition to the monetary value of selling their data, Plaintiff and Class and Subclass members also assign value to keeping their Private Data private. It is possible to quantify this privacy value, which is destroyed when Defendants intercept and collect Plaintiff's and Class and Subclass members' Private Data without notice or authorization.

69. Plaintiff and Class and Subclass members were harmed when Defendants took their property and exerted exclusive control over it, intercepting and

collecting it without Plaintiff's and Class and Subclass members' knowledge to benefit Defendants and, additionally, for still undisclosed purposes.

70. Further, Defendants' control over these ever-expanding digital dossiers makes tracking and profiling Plaintiff and Class and Subclass members, and targeting them with advertising, much more efficient and effective. Defendants unjustly earn substantial profits from such targeted advertising and/or from the sale of user data and/or information or services derived from such data.

71. In sum, Defendants have intercepted and collected Plaintiff's and Class and Subclass members' Private Data without providing anything of value to Plaintiff and Class and Subclass members in exchange for that Private Data. Moreover, Defendants' unauthorized access to Plaintiff's and Class and Subclass members' Private Data has diminished the value of that Private Data. These actions and omissions by Defendants have resulted in harm to Plaintiff and Class and Subclass members.

V. TOLLING OF THE STATUTE OF LIMITATIONS

72. Each unauthorized transmission of Private Data to TikTok by the TikTok SDK is a separate "wrong" which triggers anew the relevant statute of limitations.

73. Moreover, any applicable statute of limitations has been tolled under (1) the fraudulent concealment doctrine, based on Defendants' knowing and active concealment and denial of the facts alleged herein, and (2) the delayed discovery doctrine, as Plaintiff and Class and Subclass members did not and could not reasonably have discovered Defendants' conduct alleged herein until shortly before the filing of this Complaint. Plaintiff and Class and Subclass members did not discover and could not reasonably have discovered that Defendants were intercepting, collecting, saving, and using their Private Data in the ways set forth in this Complaint until shortly before the lawsuit was filed in consultation with counsel.

VI. NAMED PLAINTIFF ALLEGATIONS

74. Plaintiff Bernadine Griffith is a resident of Riverside County, California. Ms. Griffith has never been a registered user of the TikTok app or held any TikTok account. She made a conscious decision not to do so because, like many other Americans, she was concerned that TikTok would violate her privacy.

75. Unbeknownst to Ms. Griffith, several of the non-TikTok websites that she frequently visited have installed the TikTok SDK. TikTok secretly intercepted and collected her Private Data from these websites through the TikTok SDK, including browsing history and search queries. This is precisely what Ms. Griffith wanted to avoid when she chose not to become a registered user of the TikTok app or hold any TikTok account.

76. For example, since 2017, Ms. Griffith has from time to time subscribed to the video streaming service Hulu to watch her favorite television shows. Ms. Griffith visited Hulu frequently, and had done so as recently as the past month. The TikTok SDK was and is installed on Hulu. Thus, unbeknownst to Ms. Griffith, when she visited Hulu, TikTok stole her Private Data through the TikTok SDK. This includes information on what videos she searched for, browsed, and watched.

77. Since June 2018, Ms. Griffith has been a member of the e-commerce website Etsy. Ms. Griffith visited Etsy frequently, and had done so as recently as the past month. The TikTok SDK was and is installed on Etsy. Thus, unbeknownst to Ms. Griffith, when she visited Etsy, TikTok stole her Private Data through the TikTok SDK. This includes information on what products she searched for, browsed, purchased, and sold.

78. In or around early 2022, Ms. Griffith visited Build-a-Bear Workshop, a website that sells custom-made Teddy Bears. The TikTok SDK was and is installed on Build-a-Bear Workshop. Thus, unbeknownst to Ms. Griffith, every time she visited Build-a-Bear Workshop, TikTok stole her Private Data through the TikTok SDK. This includes information on what products she searched for, browsed,

purchased, and sold.

79. Ms. Griffith is very conscious about her online privacy. She is a user of the Microsoft Edge and Google Chrome browsers. On both browsers, Ms. Griffith has changed her settings to block third-party cookies and has enabled the "do not track" function. She also utilizes McAfee security software to protect her online privacy. Despite Ms. Griffith's efforts, the TikTok SDK circumvents these measures and obtains her Private Data, by among other things transmuting its third-party cookie into a first-party cookie.

80. These websites – Hulu, Etsy, and Build-a-Bear Workshop – are just some representative examples of websites where TikTok has stolen the Private Data of Ms. Griffith and Class and Subclass members. Upon information and belief, the TikTok SDK is installed on at least hundreds if not thousands of websites, including many popular websites visited on a day-to-day basis by millions of Americans including Ms. Griffith and Class and Subclass members.

VII. CLASS ALLEGATIONS

81. Plaintiff incorporates by reference all foregoing allegations.

82. Pursuant to Federal Rule of Civil Procedure 23 ("Rule 23"), Plaintiff seeks to represent the following classes:

> **The First Nationwide Class**: All natural persons residing in the United States who visited a website with the TikTok SDK software installed during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.
>
> **The First California Subclass**: All natural persons residing in the state of California who visited a website with the TikTok SDK software installed during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account.
>
> **The Nationwide Cookie Blocking Class**: All natural persons residing in the United States who visited a website with the TikTok SDK software

> installed during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account, and had web browser or system settings turned on to block third-party cookies.
>
> **The California Cookie Blocking Subclass**: All natural persons residing in the state of California who visited a website with the TikTok SDK software installed during the Class Period, and who have never been registered users of the TikTok app or held any TikTok account, and had web browser or system settings turned on to block third-party cookies.

83. The Class Period begins on the date that Defendants first received Private Data from non-TikTok users of websites on which the TikTok SDK was and/or is installed, as a result of the TikTok SDK, and continues through the present.

84. Plaintiff reserves the right to modify or refine the definitions of the First Nationwide Class, the First California Subclass, the Nationwide Cookie Blocking Class, and the California Cookie Blocking Subclass based upon discovery of new information and to accommodate any of the Court's manageability concerns.

85. Excluded from the Classes and Subclasses are: (i) any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; (ii) Defendants, Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) counsel for Plaintiff and Defendants; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

86. **Numerosity (Rule 23(a)(1)).** The Classes and Subclasses are so numerous that joinder of individual members therein is impracticable. The exact number of Class and Subclass members, as herein identified and described, is not

known, but each of the websites cited as illustrative examples in this Complaint are known to have millions of users based on publicly-available data.

87. **Commonality (Rule 23(a)(2))**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class and Subclass members, including the following:

(a) Whether Defendants used the TikTok SDK to read, attempt to read, learn, attempt to learn, eavesdrop, record, use, intercept, receive, and/or collect electronic communications of Private Data from Plaintiff and Class and Subclass members during the Class Period;

(b) Whether Defendants' practice of using the TikTok SDK to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic communications of Private Data from Plaintiff and Class and Subclass members during the Class Period, violates the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.*;

(c) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiff and Class and Subclass members through the TikTok SDK violates the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*;

(d) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiff and Class and Subclass members through the TikTok SDK violates Cal. Pen. Code §§ 484, 496;

(e) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiff and Class and Subclass members through the TikTok SDK constitutes conversion under California law;

(f) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiff and

Class and Subclass members through the TikTok SDK violates the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*;

(g) Whether Defendants' practice of intercepting, receiving, and/or collecting electronic communications of Private Data from Plaintiff and Class and Subclass members through the TikTok SDK violates the California Constitution and/or qualifies as an intrusion upon seclusion under California law;

(h) Whether Defendants sold Private Data or access to Private Data unlawfully obtained from Plaintiff and Class and Subclass members through the TikTok SDK;

(i) Whether Plaintiff and Class and Subclass members sustained damages as a result of Defendants' alleged conduct, and, if so, what is the appropriate measure of damages and/or restitution; and

(j) Whether Plaintiff and Class and Subclass members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein.

88. **Typicality (Rule 23(a)(3))**. Plaintiff's claims are typical of the claims of members of the Classes and Subclasses because, among other things, Plaintiff and members of the Classes and Subclasses sustained similar injuries as a result of Defendants' uniform wrongful conduct and their legal claims all arise from the same events and wrongful conduct by Defendants.

89. **Adequacy (Rule 23(a)(4)):** Plaintiff will fairly and adequately protect the interests of the Classes and Subclasses. Plaintiff's interests do not conflict with the interests of the Classes and Subclasses, and Plaintiff has retained counsel with experience in complex class actions, as well as sufficient financial and legal resources to prosecute this case on behalf of the Classes and Subclasses. Plaintiff and her counsel have no interest that is in conflict with, or otherwise antagonistic to the

interests of the other Class and Subclass members. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes and Subclasses. Plaintiff anticipates no difficulty in the management of this litigation as a class action.

90. **Predominance & Superiority (Rule 23(b)(3)):** In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members of the Classes and Subclasses, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. Here, common issues predominate because liability can be determined on a class-wide basis, even where some individualized damages determination may be required. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by complex legal and factual issues of the case to all parties and the court system. Furthermore, the expense and burden of individual litigation make it impossible for Class and Subclass members to individually redress the wrongs done to them. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VIII. CALIFORNIA LAW APPLIES TO ALL THE CLASSES AND SUBCLASSES

91. California substantive law applies to Plaintiff and every member of the Classes and Subclasses. California substantive law may be constitutionally applied to the claims of Plaintiff and Class and Subclass members under the Due Process Clause, 14th Amend. § 1, and the Full Faith and Credit Clause, Art. IV. § 1 of the U.S. Constitution. California has significant contacts, or significant aggregation of contacts, to the claims asserted by Plaintiff and Class and Subclass members, thereby

creating state interests to ensure that the choice of California state law is not arbitrary or unfair.

92. Defendants' principal place of business is in California and Defendant TikTok, Inc. is a California corporation. Given Defendants' substantial business in California, California has an interest in regulating their conduct under its laws. Given Defendants' decision to avail themselves of California's laws, the application of California law to the claims herein is constitutionally permissible.

IX. CAUSES OF ACTION

FIRST CAUSE OF ACTION

(Violation of the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq.* – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

93. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

94. The California Invasion of Privacy Act ("CIPA"), codified at Cal. Pen. Code §§ 630-638, begins by providing its statement of purpose:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

Cal. Pen. Code § 630.

95. Cal. Pen. Code § 631(a) imposes liability upon:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner . . . willfully and ***without the consent of all parties*** to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section . . . . [Emphasis added.]

96. Cal. Pen. Code § 632(a) imposes liability upon:

> A person who, intentionally and ***without the consent of all parties*** to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio [Emphasis added.]

97. Under either section of the CIPA quoted above, a defendant must show it had the consent of all parties to a communication.

98. Defendants knowingly and intentionally used and continue to use the TikTok SDK and receiving servers (where the Private Data was and is saved and recorded), both of which are recording devices under CIPA, to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic communications containing Private Data from Plaintiff and Class and Subclass members, while these electronic communications were and are in transit, originating in or sent to California, and without the authorization or consent of Plaintiff, Class members, or Subclass members.

99. Plaintiff and Subclass members were and are in California during one or more of the instances where Defendants intercepted their communications. Upon information and belief, each Class and Subclass member, even those located outside of California, during one or more of their interactions on the Internet during the applicable statute of limitations period, communicated with one or more entities based in California, and/or with one or more entities whose servers were located in California. Communications from the California web-based entities to Class and Subclass members were sent from California. Communications to the California web-based entities from Class and Subclass members were sent to California.

100. The communications intercepted by Defendants include "contents" of electronic communications exchanged between Plaintiff and Class and Subclass members, on the one hand, and the websites where the TikTok SDK was installed, on the other, in the form of detailed URL requests, webpage browsing histories and

search queries, and URLs containing the specific search queries. Defendants' non-consensual interception of these communications was designed to learn at least some of these contents.

101. The following items constitute "machine[s], instrument[s], or contrivance[s]" under Cal. Penal Code § 631(a), and even if they did not, Defendants' purposeful scheme that facilitated its interceptions falls under the broad statutory catch-all category of "any other manner":

(a) Plaintiff's and Class and Subclass members' browsers;

(b) Plaintiff's and Class and Subclass members' personal computing devices;

(c) the computer codes and programs used by Defendants to effectuate the interception of communications exchanged between websites and search engines, on the one hand, and Plaintiff and Class and Subclass members, on the other;

(d) Defendants' servers, at least some of which, on information and belief, are located in California;

(e) the servers of the third-party websites from which Defendants' intercepted Plaintiff's and Class and Subclass members' communications;

(f) the plan Defendants carried out to effectuate the interception of the communications that were exchanged between the third-party websites, on the one hand, and Plaintiff and Class and Subclass members, on the other.

102. The Private Data collected by Defendants constituted "confidential communications," as that term is used in Cal. Pen. Code § 632(a), because Plaintiff and Class and Subclass members have an objectively reasonable expectation of privacy that their private browsing communications are not being intercepted, collected or disseminated by Defendants – particularly given that Plaintiff and Class

and Subclass members had never been registered users of the TikTok app or held any TikTok accounts.

103. Plaintiff and Class and Subclass members have suffered loss because of these violations, including, but not limited to, violation of their rights to privacy and loss of value in their Private Data.

104. Pursuant to Cal. Pen. Code § 637.2, Plaintiff and Class and Subclass members have been injured by the violations of Cal. Pen. Code §§ 631, 632, and each seeks damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive or other equitable relief.

SECOND CAUSE OF ACTION

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

105. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

106. Plaintiff's and Class and Subclass members' devices used to access the third-party websites are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B). Plaintiff's and Class and Subclass members' Internet browsing, which Defendants impermissibly tracked, involved submissions to websites for companies all over the United States, both for purchases of goods and information.

107. Defendants have exceeded, and continue to exceed, authorized access to Plaintiff's and Class and Subclass members' protected computers and obtained information from them, in violation of 18 U.S.C. § 1030(a)(2).

108. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiff's and Class and Subclass members' Private Data – including webpage browsing histories

and search queries, and URLs containing the specific search queries.

109. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally-identifiable data and content of Plaintiff and Class and Subclass members being made available to foreign actors, potentially including foreign intelligence services, in locations without adequate legal privacy protections. That this threat is real and imminent is evidenced by the ban on use of the TikTok app by federal employees, as well as proposed legislation that would ban domestic use of the TikTok app entirely.

110. Accordingly, Plaintiff and Class and Subclass members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

THIRD CAUSE OF ACTION

(Statutory Larceny, Cal. Pen. Code §§ 484, 496 – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

111. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

112. Cal. Pen. Code § 496 imposes liability upon:

> [e]very person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained[.]

113. Cal. Pen. Code § 484, which defines "theft", states in pertinent part:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

114. Under California law, Plaintiff's and Class and Subclass members' Private Data constitutes property that can be the subject of theft.

115. Defendants acted in a manner constituting theft by surreptitiously taking Plaintiff's and Class and Subclass members' Private Data through the TikTok SDK installed on third-party websites, with the specific intent to deprive Plaintiff and Class and Subclass members of their property.

116. Plaintiff and Class and Subclass members did not consent to any of Defendants' actions in taking Plaintiff's and Class and Subclass members' Private Data.

117. Pursuant to Cal. Pen. Code § 496(c), Plaintiff and Class and Subclass members are entitled to treble damages, as well as attorneys' fees and costs, for injuries sustained as a result of Defendants' violations of Cal. Pen. Code § 496(a).

FOURTH CAUSE OF ACTION

(Conversion – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

118. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

119. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things such as data or communications. Plaintiff's and Class and Subclass members' Private Data is their property under California law.

120. Defendants unlawfully intercepted, collected, used, and exercised dominion and control over Plaintiff's and Class and Subclass members' Private Data without authorization.

121. Defendants wrongfully exercised control over Plaintiff's and Class and Subclass members' Private Data, and have not returned such Private Data.

122. Plaintiff and Class and Subclass members have been damaged as a result of Defendants' unlawful conversion of their property.

FIFTH CAUSE OF ACTION

(Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

123. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

124. California's Unfair Competition Law ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code §17200.

125. Defendants engaged in "unlawful" conduct through their violation of state and federal law, including (a) violation of the California Invasion of Privacy Act, Cal. Pen. Code § 630 *et seq*.; (b) violation of the Computer Fraud and Abuse Act**,** 18 U.S.C. § 1030 *et seq*.; (c) violation of Cal. Pen. Code §§ 484, 496; (d) conversion; (e) invasion of privacy under Article I, Section 1 of the California Constitution; and (f) intrusion upon seclusion.

126. Defendants engaged in "unfair" conduct, because they knowingly intercepted and collected communications, and/or knowingly received intercepted communications, containing the Private Data of Plaintiff and Class and Subclass members under circumstances in which Plaintiff and Class and Subclass members would have no reason to know that such information was being intercepted because it was never disclosed or otherwise made known to them by Defendants.

127. Plaintiff and Class and Subclass members have suffered injury-in-fact, including the loss of money and/or property as a result of Defendants' unfair and/or unlawful practices, to wit, the unauthorized collection of their Private Data, which has value in an amount to be proven at trial. Moreover, Plaintiff and Class and Subclass members have suffered harm in the form of diminution of the value of their Private Data.

128. Defendants' actions caused damage to and loss of Plaintiff's and Class and Subclass members' property right to control the dissemination and use of their

Private Data.

129. Defendants have taken property from Plaintiff and Class and Subclass members without providing just, or any, compensation.

130. Defendants should be required to cease their unfair and/or illegal collection of user data and to retrieve and delete all unfairly and/or illegally obtained user data. Defendants reaped unjust profits and revenues in violation of the UCL. Plaintiff and Class and Subclass members seek injunctive relief governing Defendants' ongoing taking and possession of their Private Data, and/or failure to account to Plaintiff and Class and Subclass members concerning Defendants' interception, collection, possession, and use of Plaintiff's and Class and Subclass members' Private Data, and restitution and disgorgement of resulting unjust profits and revenues to Defendants.

131. Plaintiff and Class and Subclass members lack an adequate remedy at law because the ongoing harms from Defendants' interception, collection, taking, possession, and use of Private Data must be addressed by injunctive relief and, due to the ongoing and nature of the harm, the harm cannot be adequately addressed by monetary damages alone.

SIXTH CAUSE OF ACTION

(Invasion of Privacy under Article I, Section 1 of the California Constitution – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

132. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

133. In 1972, California added a right of privacy to the list of enumerated inalienable rights in Article I, Section 1 of its Constitution.

134. The right to privacy was added to the California Constitution after voters approved a legislative constitutional amendment designated as Proposition 11. Critically, the argument in favor of Proposition 11 reveals that the legislative intent was to curb businesses' control over the unauthorized collection and use of

consumers' personal information, stating:

> The right to privacy is the right to be left alone . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulating of personal information. This is essential to social relationships and personal freedom.[40]

135. The principal purpose of this Constitutional right was to protect against unnecessary information gathering, use, and dissemination by public and private entities, including Defendants.

136. The right to privacy in California's Constitution creates a right of action against private entities like the Defendants.

137. To plead invasion of privacy under the California Constitution, Plaintiff and Class and Subclass members must allege "that (1) they possess a legally protected privacy interest, (2) they maintain a reasonable expectation of privacy, and (3) the intrusion is 'so serious . . . as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020), quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009).

138. Plaintiff and Class and Subclass members have a legally protected privacy interest in (a) precluding the interception, collection, copying, dissemination and/or misuse of their Private Data; and (b) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without having that information intercepted and transmitted to Defendants without Plaintiff's and Class and Subclass members' knowledge or consent.

139. Plaintiff and Class and Subclass members have a reasonable expectation of privacy in the Private Data that Defendants intercept and collect without adequate

[40] BALLOT PAMP., PROPOSED STATS. & AMENDS. TO CAL. CONST. WITH ARGUMENTS TO VOTERS, GEN. ELECTION *26 (NOV. 7, 1972).

notice or consent – particularly given that Plaintiff and Class and Subclass members had never been registered users of the TikTok app or held any TikTok accounts.

140. Defendants' actions constitute a serious invasion of privacy in that they: (a) invade a zone of privacy protected by the Fourth Amendment, namely, the right to privacy in data contained on personal computing devices, including web search and browsing histories; (b) violate federal criminal laws including the Computer Fraud and Abuse Act; and (c) invade the privacy interests and rights of millions of U.S. residents (including Plaintiff and Class and Subclass members) without their consent.

141. Defendants' surreptitious and unauthorized interception and collection – through the TikTok SDK installed on third-party websites – of the internet communications of millions of U.S. residents who have made the conscious decision not to interact with Defendants or the TikTok app constitutes an egregious breach of social norms that is highly offensive. This behavior is doubly offensive because the Private Data intercepted and collected is paired with other secretly collected data, such as data collected from multiple websites installed with the TikTok SDK, resulting in Defendants creating digital dossiers of individuals. This conduct is even more offensive where Defendants evade the browser or system settings in place to block third-party tracking.

142. Defendants lacked a legitimate business interest in intercepting and receiving private internet communications between Plaintiff and Class and Subclass members, on the one hand, and the third-party websites with the TikTok SDK installed, on the other, without first obtaining the consent of Plaintiff and Class and Subclass members.

143. Plaintiff and Class and Subclass members have sustained, and will continue to sustain, damages as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation and injunctive relief, as well as such other relief as the Court may deem just and proper.

SEVENTH CAUSE OF ACTION

(Intrusion Upon Seclusion – By Plaintiff, the Classes, and the Subclasses Against All Defendants)

144. Plaintiff, individually and on behalf of the Classes and Subclasses, incorporates the foregoing allegations as if fully set forth herein.

145. A claim for intrusion upon seclusion requires (1) intrusion into a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

146. By intercepting the internet communications of Plaintiff and Class and Subclass members, on one hand, and third-party websites with the TikTok SDK installed, on the other, Defendants intentionally intruded upon the solitude and/or seclusion of Plaintiff and Class and Subclass members.

147. Defendants' intrusion was intentional. Defendants intentionally designed the TikTok SDK and underlying programming code to surreptitiously intercept, collect, and retain the Private Data of Plaintiff and Class and Subclass members. Defendants effectively place themselves in the middle of conversations. Defendants also intentionally intruded upon Plaintiff's and Class and Subclass members' solitude, seclusion, and private affairs by intentionally receiving and using this Private Data for their own benefit, knowing how it had been obtained.

148. Defendants intercept these internet communications containing Private Data without authority or consent from Plaintiff or Class and Subclass members.

149. Defendants' intentional intrusion into Plaintiff's and Class and Subclass members' internet communications, computing devices, and web browsers is highly offensive to a reasonable person in that such intrusions violate federal and state criminal and civil laws designed to protect individual privacy and guard against theft. Such behavior is doubly offensive because the Private Data intercepted and collected is paired with other secretly collected data from other websites with the TikTok SDK installed, allowing Defendants to create unique digital dossiers. This conduct is even

more offensive where Defendants evade the browser or system settings in place to block third-party tracking.

150. Plaintiff and Class and Subclass members reasonably expected that their Private Data would not be intercepted, collected, stored, or used by Defendants, particularly given that Plaintiff and Class and Subclass members had never been registered users of the TikTok app or held any TikTok accounts.

151. Plaintiff and Class and Subclass members have sustained, and will continue to sustain, damages as a direct and proximate result of Defendants' intrusions and are entitled to just compensation and injunctive relief, as well as such other relief as the Court may deem just and proper.

152. Plaintiff and Class and Subclass members have been damaged by these intrusions, which have allowed Defendants to obtain profits that rightfully belong to Plaintiff and Class and Subclass members. Plaintiff and Class and Subclass members are entitled to reasonable compensation including but not limited to disgorgement of profits related to the unlawful intrusion into their private internet communications.

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests relief against Defendants as set forth below:

a. Certifying the proposed Classes and Subclasses as requested herein pursuant to Federal Rule of Civil Procedure 23;

b. Entering an order appointing Plaintiff as representative of the Classes and Subclasses;

c. Entering an order appointing undersigned counsel to represent the Classes and Subclasses;

d. Entering Judgment in favor of each Class and Subclass member for damages suffered as a result of the conduct alleged herein, as well as punitive damages, restitution, disgorgement, the greater of $5,000 or three times the amount of actual damages pursuant to Cal. Pen. Code §

637.2, and treble damages pursuant to Cal. Pen. Code § 496, including interest and prejudgment interest;

e. Entering an order granting injunctive relief as permitted by law or equity, including enjoining Defendants from continuing any unlawful practices as set forth herein, and directing Defendants to identify, with Court supervision, victims of their conduct and pay them all the money they are required to pay;

f. Awarding Plaintiff and Class and Subclass members their reasonable costs and expenses incurred in this action, including attorneys' fees and costs;

g. Ordering that Defendants delete the Private Data that they intercepted and collected from Plaintiff and Class and Subclass members; and

h. Providing any such further relief as the Court deems just and proper.

XI. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

DATED: May 26, 2023

Ekwan E. Rhow
Marc E. Masters
Christopher J. Lee
BIRD, MARELLA, BOXER, WOLPERT, NESSIM, DROOKS, LINCENBERG & RHOW, P.C.

By: /s/ Ekwan E. Rhow
Ekwan E. Rhow
Attorneys for Plaintiff Bernadine Griffith

DATED: May 26, 2023

Jonathan M. Rotter
Kara M. Wolke
Gregory B. Linkh
GLANCY PRONGAY & MURRAY LLP

By: /s/ Jonathan M. Rotter
Jonathan M. Rotter
Attorneys for Plaintiff Bernadine Griffith

DATED: May 26, 2023

Kalpana Srinivasan
Steven Sklaver
Michael Gervais
SUSMAN GODFREY L.L.P.

By: /s/ Michael Gervais
Michael Gervais
Attorneys for Plaintiff Bernadine Griffith

ATTESTATION

Pursuant to L.R. 5-4.3.4, the filer attests that all signatories listed, and on whose behalf this filing is submitted, concur in its content and have authorized the filing.

DATED: May 26, 2023

Ekwan E. Rhow
Marc E. Masters
Christopher J. Lee
Bird, Marella, Boxer, Wolpert, Nessim,
Drooks, Lincenberg & Rhow, P.C.

By: Ek Rhow

Ekwan E. Rhow
Attorneys for Plaintiff Bernadine Griffith